

(19)



JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **03113657 A**

(43) Date of publication of application: **15 . 05 . 91**

(51) Int. Cl. **G06F 12/14**
G06F 9/06
G09C 1/00

(21) Application number: **01253273**

(22) Date of filing: **28 . 09 . 89**

(71) Applicant: **NEC CORP HOKKAIDO NIPPON
DENKI SOFTWARE KK**

(72) Inventor: **SEKINE MASAOKI
KAMOI ISAO**

(54) INFORMATION ACCUMULATION EXCHANGE/SECURITY CONTROL SYSTEM

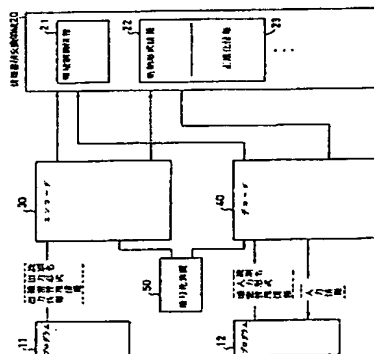
(57) Abstract:

PURPOSE: To prevent a processing from becoming complicated by providing the program with unified means for outputting and inputting information to be accumulated and exchanged and a means controlling the security of information.

CONSTITUTION: When the program 11 declares the output system of information and security control information and outputs information, an encoder 30 generates storage type information 22 from an output system, converts information into normalization information in accordance with storage type information, stores it in an information accumulation exchange area 20 and stores storage type information 22 with ciphering information 24 in the information accumulation exchange area 20. If security control information obtained by decoding ciphering information by a prescribed ciphering device and security control information which the program 12 declares are referred and they coincide when the program 12 requests the input of information, normalization information stored in the information accumulation exchange area is converted in accordance with storage type information and an input system while it is inputted to the program 12. Thus, the processing

when information is accumulated and exchanged between multiple different programs is prevented from becoming complicated.

COPYRIGHT: (C)1991,JPO&Japio



⑯ 公開特許公報(A)

平3-113657

⑮ Int. Cl.

識別記号

庁内整理番号

⑰ 公開 平成3年(1991)5月15日

G 06 F 12/14

3 2 0 B

7737-5B

9/06

4 5 0 G

7361-5B

G 09 C 1/00

7343-5B

審査請求 未請求 請求項の数 1 (全10頁)

⑱ 発明の名称 情報蓄積交換・機密管理方式

⑲ 特 願 平1-253273

⑳ 出 願 平1(1989)9月28日

㉑ 発 明 者 関 根 正 明 北海道札幌市中央区大通西4丁目1番地 北海道日本電気
ソフトウェア株式会社内

㉒ 発 明 者 鴨 井 功 東京都港区芝5丁目33番1号 日本電気株式会社内

㉓ 出 願 人 日本電気株式会社 東京都港区芝5丁目7番1号

㉔ 出 願 人 北海道日本電気ソフトウエア株式会社 北海道札幌市中央区大通西4丁目1番地

㉕ 代 理 人 弁理士 河原 純一

明 細 書

1. 発明の名称

情報蓄積交換・機密管理方式

2. 特許請求の範囲

互いに独立した複数のプログラムが実行される電子計算機システムのプログラム間の情報蓄積交換・機密管理方式において、

前記プログラム間で蓄積および交換される情報を格納する情報蓄積交換領域と、

第1のプログラムが前記情報の出力形式および機密管理情報を宣言して前記情報を出力したときに前記出力形式から格納形式情報を生成しこの格納形式情報に従って前記情報を正規化情報に変換して前記情報蓄積交換領域に格納するとともに前記格納形式情報を前記機密管理情報を所定の暗号化装置により暗号化した暗号化情報とともに前記情報蓄積交換領域に記録するエンコードと、

第2のプログラムが前記情報の入力形式および機密管理情報を宣言して前記情報を入力要求したときに前記暗号化情報を所定の暗号化装置により

解読した機密管理情報と第2のプログラムが宣言した機密管理情報とを照合して一致した場合に前記情報蓄積交換領域に格納された正規化情報を前記格納形式情報と前記入力形式とに従って変換しながら第2のプログラムに入力させるデコードとを有することを特徴とする情報蓄積交換・機密管理方式。

3. 発明の詳細な説明

〔産業上の利用分野〕

本発明は情報蓄積交換・機密管理方式に関し、特に互いに独立な複数のプログラムが実行される電子計算機システムにおいて複数のプログラム間で情報の蓄積および交換を行う情報蓄積交換・機密管理方式に関する。

〔従来の技術〕

従来、複数のプログラム間で情報の蓄積および交換を行う場合、情報の送り手側のプログラムが受け手側のプログラムの情報の入力形式に一致させて情報を変換しながら出力する方式、情報の受け手側のプログラムが送り手側のプログラムの情

報の出力形式に一致させて情報を変換しながら入力する方式、または送り手側のプログラムと受け手側のプログラムとの間に第3のプログラムを介在させて前者の出力形式に従って出力された情報を後者の入力形式に一致する形式に変換する方式のいずれかが採用されてきた。

(発明が解決しようとする課題)

上述した従来の複数のプログラム間で情報の蓄積および交換を行う方式では、情報の出力形式および情報の入力形式は送り手側のプログラムおよび受け手側のプログラムのいずれか一方または双方に依存した形式となるので、以下に挙げるような欠点がある。

① 多数の異なったプログラムとの間で情報の蓄積および交換を行うプログラムの場合、相手側の個々のプログラムのそれぞれに対応する変換処理を組み込まなければならない、処理が複雑になる。

② 情報の蓄積および交換を行う相手側のプログラムが増加した場合にそれに対応してプログラムを修正しなければならない。

号化装置により暗号化した暗号化情報とともに前記情報蓄積交換領域に記録するエンコードと、第2のプログラムが前記情報の入力形式および機密管理情報を宣言して前記情報を入力要求したときに前記暗号化情報を所定の暗号化装置により解読した機密管理情報と第2のプログラムが宣言した機密管理情報とを照合して一致した場合に前記情報蓄積交換領域に格納された正規化情報を前記格納形式情報と前記入力形式とに従って変換しながら第2のプログラムに入力させるデコードとを有する。

(作用)

本発明の情報蓄積交換・機密管理方式では、情報蓄積交換領域がプログラム間で蓄積および交換される情報を格納し、エンコードが第1のプログラムが情報の出力形式および機密管理情報を宣言して情報を出力したときに出力形式から格納形式情報を生成し格納形式情報に従って情報を正規化情報に変換して情報蓄積交換領域に格納するとともに格納形式情報を機密管理情報を所定の暗号化

③ 情報の保護が十分に行われていないために、情報の出力形式を認知すれば自由に参照でき、情報の漏洩が発生する。

本発明の目的は、上述の点に鑑み、蓄積および交換される情報を出力および入力するための統一的手段と情報の機密管理を行う手段とをプログラムに与えるようにした情報蓄積交換・機密管理方式を提供することにある。

(課題を解決するための手段)

本発明の情報蓄積交換・機密管理方式は、互いに独立した複数のプログラムが実行される電子計算機システムのプログラム間の情報蓄積交換・機密管理方式において、前記プログラム間で蓄積および交換される情報を格納する情報蓄積交換領域と、第1のプログラムが前記情報の出力形式および機密管理情報を宣言して前記情報を出力したときに前記出力形式から格納形式情報を生成しこの格納形式情報に従って前記情報を正規化情報に変換して前記情報蓄積交換領域に格納するとともに前記格納形式情報を前記機密管理情報を所定の暗

号化装置により暗号化した暗号化情報とともに情報蓄積交換領域に記録し、デコードが第2のプログラムが情報の入力形式および機密管理情報を宣言して情報を入力要求したときに暗号化情報を所定の暗号化装置により解読した機密管理情報と第2のプログラムが宣言した機密管理情報とを照合して一致した場合に情報蓄積交換領域に格納された正規化情報を格納形式情報と前記入力形式とに従って変換しながら第2のプログラムに入力させる。

(実施例)

次に、本発明について図面を参照して詳細に説明する。

第1図は、本発明の一実施例に係る情報蓄積交換・機密管理方式が適用された電子計算機システムの構成を示すブロック図である。この電子計算機システムは、互いに独立なプログラム11およびプログラム12と、それらの間で蓄積および交換される情報を格納するための情報蓄積交換領域20と、プログラム11が情報の出力形式等を宣言して蓄積および交換される情報を書き出したと

きに蓄積および交換される情報を格納形式情報22および正規化情報23に変換して情報蓄積交換領域20に出力するエンコード30と、プログラム12が情報の入力形式等を宣言して蓄積および交換される情報を読み込もうとしたときに情報蓄積交換領域20に格納された格納形式情報22および正規化情報23を入力形式に含わせて変換してプログラム12に入力させるデコード40とを含んで構成されている。

情報蓄積交換領域20には、プログラム11および12間で蓄積および交換される情報の格納形式および内容を示す格納形式情報22および正規化情報23と、格納形式情報22および正規化情報23が情報の蓄積および交換を行うプログラムの組に応じて複数個存在し得るのでこれらを管理するための領域制御情報21とが格納される。

プログラム11が出力した蓄積および交換される情報は、エンコード30が格納形式情報22および正規化情報23に変換して情報蓄積交換領域20に格納する。

識別名記録有無判定ステップ401と、機密情報一致判定ステップ402と、格納域ポインタ取得ステップ403と、格納形式情報参照ステップ404と、入力形式情報生成ステップ405と、命令群構成ステップ406と、入力情報生成ステップ407と、入力形式情報および入力情報転送ステップ408と、入力情報生成完了通知ステップ409と、参照不可能通知ステップ410とからなる。

第5図は、デコード40によって格納形式情報22から入力形式に従って生成される入力形式情報の一例を示す図である。入力形式情報は、要求元のプログラム12が宣言した入力形式を格納形式情報22に従ってより具体化したものである。

第6図は、正規化情報23を変換して入力情報を生成するための命令群を示す図である。この命令群は、デコード40によって格納形式情報22と入力形式情報とから構成される。

第7図は、情報蓄積交換領域20に格納される領域制御情報21と格納形式情報22および正規

また、プログラム12が受け取る蓄積および交換される情報は、情報蓄積交換領域20に格納された格納形式情報22および正規化情報23をデコード40が変換したものである。

第2図を参照すると、エンコード30の処理は、識別名記録有無判定ステップ301と、格納域ポインタ取得ステップ302と、格納域初期化ステップ303と、識別名および格納域ポインタ削除ステップ304と、格納形式情報および暗号化情報生成ステップ305と、命令群構成ステップ306と、正規化情報生成ステップ307と、領域確保ステップ308と、格納形式情報および正規化情報出力ステップ309と、識別名、暗号化情報および格納域ポインタ記録ステップ310と、処理完了通知ステップ311とからなる。

第3図は、出力情報を変換して正規化情報23を生成するための命令群を示す図である。この命令群は、エンコード30によって出力形式と格納形式情報22とから構成される。

第4図を参照すると、デコード40の処理は、

化情報23との関連を例示する図である。領域制御情報21には、空領域情報と、識別名、暗号化情報24および格納域ポインタの複数の組とが格納される。格納域ポインタは、識別名で識別される格納形式情報22および正規化情報23の組を指している。

第8図は、格納形式情報22および正規化情報23の一例をそれぞれ示す図である。格納形式情報22内には、正規化情報23の格納形式が定義されている。

第9図は、プログラム11および12からの機密管理情報の与え方を例示する図である。機密管理情報は、機密情報(パスワード)と、この機密情報(パスワード)をどのような方法で暗号化するかを指示する暗号化タイプとからなる。

第10図は、情報蓄積交換領域20内の領域制御情報21に記録される暗号化情報24の出力例を示す図である。記録されている機密情報(パスワード)は、暗号化タイプ「A」で暗号化されたものであることを示している。

次に、このように構成された本実施例の情報蓄積交換・機密管理方式の動作について説明する。

プログラム11は、エンコード30に対する入力情報として、蓄積および交換される情報を識別するための識別名と、蓄積および交換される情報の出力形式および機密管理情報の宣言と、蓄積および交換される情報(出力情報)自身とを引き渡す。

エンコード30は、まず最初に、要求元のプログラム11が指定した識別名が領域制御情報21内にすでに記録されているか否かをチェックする(ステップ301)。指定された識別名が領域制御情報21内にすでに記録されている場合は、その識別名に対応して領域制御情報21に記録されている格納域ポインタを得て(ステップ302)、格納形式情報22および正規化情報23が格納されている領域を初期化し(ステップ303)、領域制御情報21内の識別名および格納域ポインタを削除する(ステップ304)。指定された識別名が領域制御情報21内に記録されていない場合

8)、格納形式情報22および正規化情報23を1組にして確保した領域に出力する(ステップ309)。

最後に、エンコード30は、領域制御情報21に、指定された識別名と、暗号化情報24と、格納形式情報22および正規化情報23を格納した領域への格納域ポインタとを記録し(ステップ310)、要求元のプログラム11に処理完了を通知する(ステップ311)。

この結果、要求元のプログラム11が出力した蓄積および交換される情報は、格納形式情報22および正規化情報23に変換されて情報蓄積交換領域20に格納される。また、格納形式情報22および正規化情報23が格納された領域を指示する格納域ポインタと、情報を識別するための識別名と、機密管理情報を暗号化した暗号化情報24とが併せて領域制御情報21内に格納される。

一方、プログラム12は、デコード40に対する入力情報として、蓄積および交換される情報を識別するための識別名と、蓄積および交換される

は、エンコード30は、ステップ302~304を実行しない。

次に、エンコード30は、要求元のプログラム11が宣言した出力形式から格納形式情報22を生成するとともに、プログラム11から与えられた機密管理情報の機密情報(パスワード)を暗号化タイプから得られる暗号化装置50により暗号化して暗号化情報24を生成する(ステップ305)。さらに、出力形式とステップ305で生成した格納形式情報22とを参照して、出力情報を変換して正規化情報23を生成するための命令群を構成する(ステップ306)。

続いて、エンコード30は、この命令群を出力情報に対して実行して正規化情報23を生成する(ステップ307)。

正規化情報23の生成後、エンコード30は、領域制御情報21を参照してステップ305で生成した格納形式情報22およびステップ307で生成した正規化情報23を格納するための領域を情報蓄積交換領域20内に確保し(ステップ30

情報の入力形式および機密管理情報の宣言と、プログラム12内の蓄積および交換される情報を受け取るための入力域の所在情報とを引き渡す。

デコード40は、まず最初に、要求元のプログラム12が指定した識別名が領域制御情報21内に記録されているか否かをチェックする(ステップ401)。指定した識別名が領域制御情報21内に記録されていない場合には、参照不可能である旨を要求元のプログラム12に通知する(ステップ410)。

また、指定した識別名が領域制御情報21内に記録されている場合には、デコード40は、プログラム12から与えられた機密管理情報の暗号化タイプを持つ暗号化装置50で機密情報(パスワード)を暗号化し、暗号化された機密情報(パスワード)と領域制御情報21内の識別名に対応する暗号化情報24の機密情報(パスワード)とを照合する(ステップ402)。照合が不正である場合には、参照不可能である旨を要求元のプログラム12に通知する(ステップ410)。

機密情報(パスワード)の照合が一致した場合は、デコード40は、識別名および暗号化情報24とともに領域制御情報21に記録されている格納域ポインタを得て(ステップ403)、格納形式情報22を参照し(ステップ404)、参照した格納形式情報22から要求元のプログラム12が宣言した入力形式に従い入力形式情報を生成する(ステップ405)。

次に、デコード40は、格納形式情報22とステップ405で生成した入力形式情報とから、正規化情報23を交換して入力情報を生成するための命令群を構成する(ステップ406)。次に、ステップ403で得た格納域ポインタを使用して正規化情報23を得て、得られた正規化情報23に対して命令群を実行して入力情報を生成する(ステップ407)。

続いて、デコード40は、要求元のプログラム12の面積および交換される情報を受け取る入力域に生成した入力情報を転送する(ステップ408)。

という欠点、

② 情報の蓄積および交換を行う相手側のプログラムが増加した場合にそれに対応してプログラムを修正しなければならないという欠点、

③ 情報の保護が十分に行われていないために、情報の出力形式を認知すれば自由に参照でき、情報の漏洩が発生するという欠点

を除去することができるという効果がある。

4. 図面の簡単な説明

第1図は本発明の一実施例に係る情報蓄積交換・機密管理方式が適用された電子計算機システムの構成を示すブロック図、

第2図は第1図中のエンコードの処理を示す流れ図、

第3図は第1図中のエンコードによって作成される命令群の一例を示す図、

第4図は第1図中のデコードの処理を示す流れ図、

第5図は要求元のプログラムが宣言した入力形式を格納形式情報に従ってより具体化した入力形

最後に、デコード40は、入力情報の生成が完了したことを要求元のプログラム12に通知する(ステップ409)。

なお、複数の計算機システムが通信回線等で結合されて1個のシステムを構成するような計算機システムにおいて、プログラム11およびプログラム12が異なった種類の中央処理装置上でそれぞれ独立に実行されているような場合でも、本発明が同様に適用できることは明白である。

(発明の効果)

以上説明したように本発明は、蓄積および交換される情報を出力および入力するための統一的な手段と情報の機密管理を行う手段とをプログラムに与えることにより、従来の複数のプログラム間で情報の蓄積および交換を行う方式の欠点、すなわち、

① 多数の異なったプログラムとの間で情報の蓄積および交換を行うプログラムの場合、相手側の個々のプログラムのそれぞれに対応する変換処理を組み込まなければならない、処理が複雑になる

式情報の一例を示す図、

第6図は第1図中のデコードによって作成される命令群の一例を示す図、

第7図は第1図中の情報蓄積交換領域に格納される領域制御情報と格納形式情報および正規化情報との関連を例示する図、

第8図は格納形式情報および正規化情報の一例を示す図、

第9図はプログラムからの機密管理情報の与え方を例示する図、

第10図は第9図の機密管理情報が暗号化された暗号化情報の一例を示す図である。

図において、

- 11・・・プログラム、
- 12・・・プログラム、
- 20・・・情報蓄積交換領域、
- 21・・・領域制御情報、
- 22・・・格納形式情報、
- 23・・・正規化情報、
- 24・・・暗号化情報、

30・・・エンコーダ、
40・・・デコーダ、
50・・・暗号化装置である。

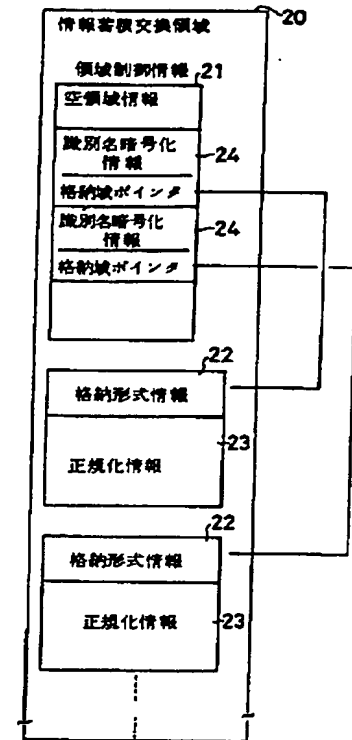
特許出願人

日 本 電 気 株 式 会 社

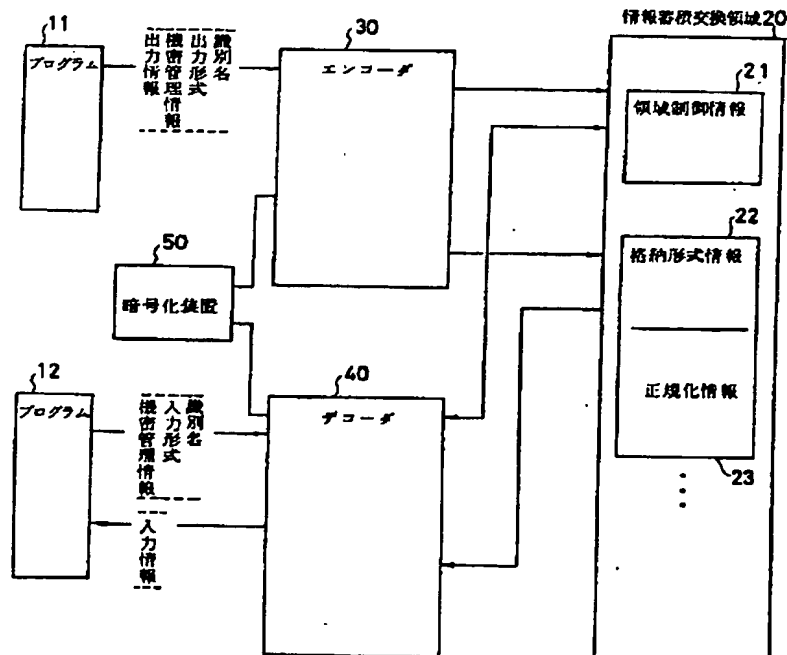
北海道日本電気ソフトウェア株式会社

代 理 人 弁 理 士 河 原 純 一

第 7 図

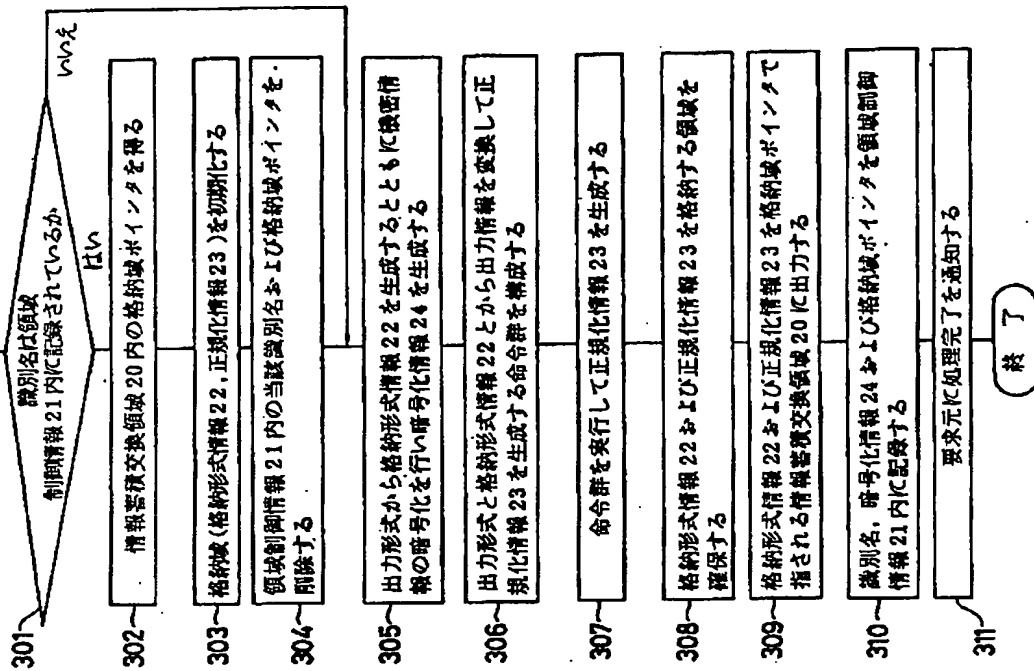


第 1 図

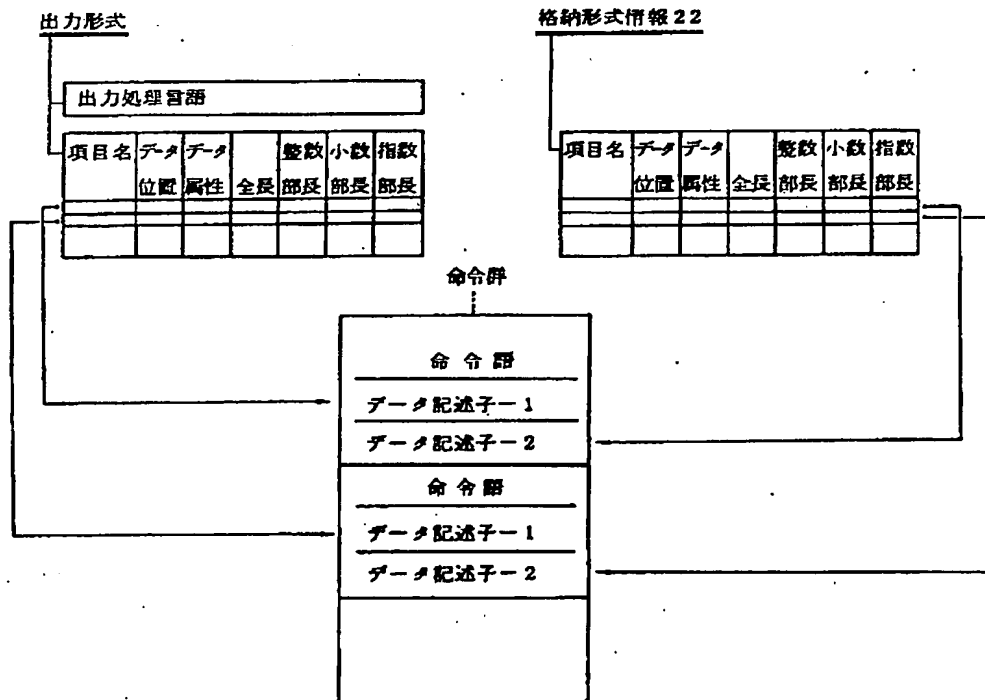


第2図

エンコード 30

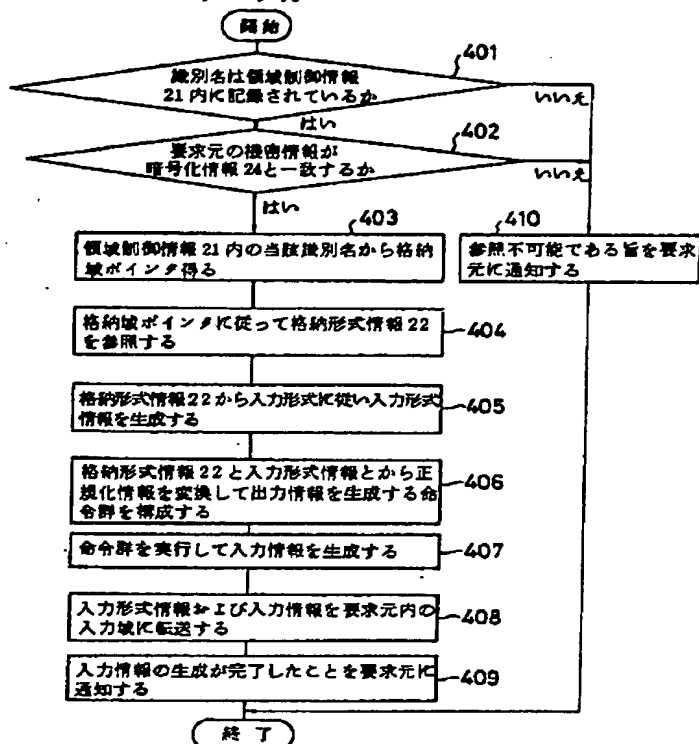


第3図

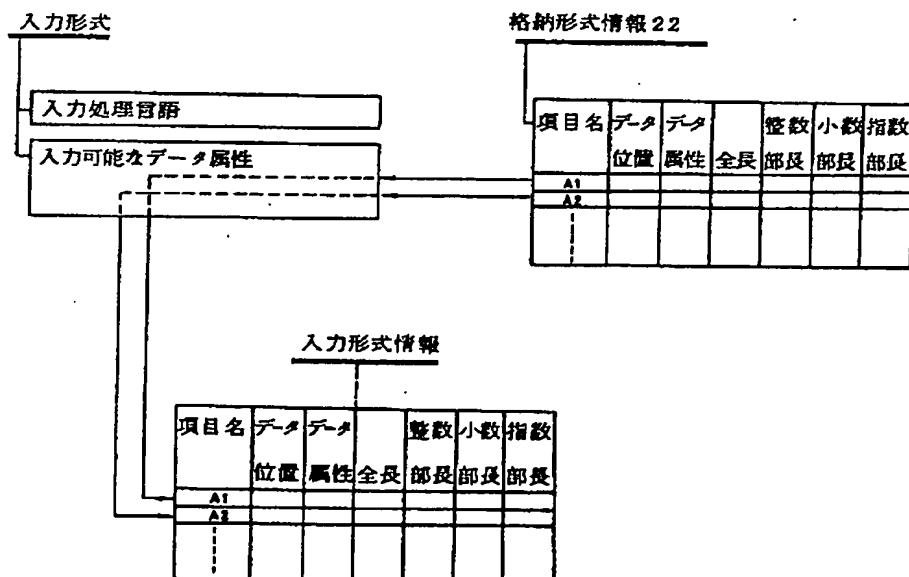


第 4 図

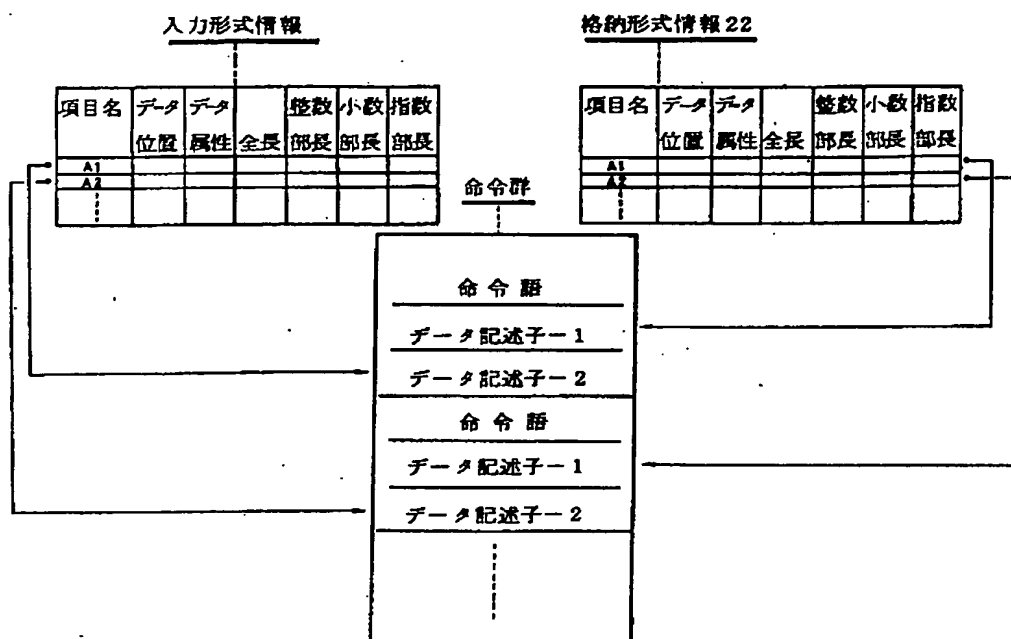
デコード 40



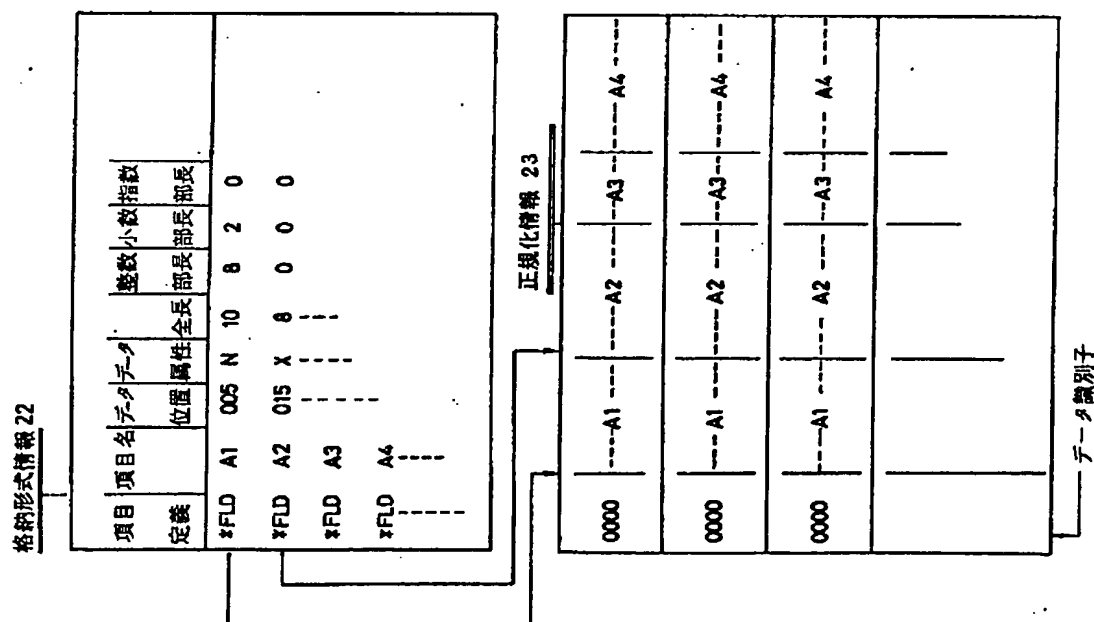
第 5 図



第 6 図



第 8 図



第 9 図

機密管理情報の与え方(プログラム11、プログラム12)

機密情報(パスワード)	=X1X2X3X4--Xn
暗号化タイプ	=A

第 10 図

暗号化情報 24

項目 定義	機密情報(パスワード)	暗号化タイプ
*OPT	xn---x4x3x2x1	A



PATENT ABSTRACTS OF JAPAN

(11) Publication number: **08055164 A**

(43) Date of publication of application: 27 . 02 . 96

(51) Int. Cl.

G06F 17/60
G06F 13/00
G09C 1/00

(21) Application number: **06219369**(22) Date of filing: **10 . 08 . 94**(71) Applicant: **FUJITSU LTD**

(72) Inventor: **AKIYAMA RYOTA**
YOSHIOKA MAKOTO

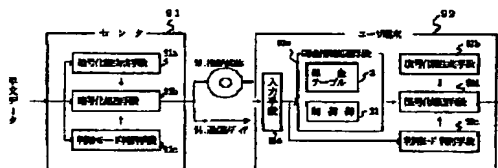
(54) **SOFTWARE DISTRIBUTION SYSTEM,
 REPEATING DEVICE, AND USER TERMINAL
 DEVICE**

(57) Abstract:

PURPOSE: To improve the security and lighten the time load on a user by selecting the best mode for the provision style of software and perform an enciphering/deciphering process on a distribution path.

CONSTITUTION: The software which is enciphered at a center 91 is offered to a user terminal 92 through a storage medium 93 or communication media 94. When the software is offered from the center 91, the user terminal 92 refers to the accounting balance of the user and allows the software to be deciphered on condition that the balance is larger than a specific value (not 0). Then the accounting balance of the user is reduced for each title of permitted software. Then the user terminal 92 generates a deciphering key on the basis of the software ID, or title, etc., of the software and also decides the mode of the software. The user terminal 92 decipheres the software on the basis of the deciphering key and mode and outputs it to an output device such as a display and a speaker.

COPYRIGHT: (C)1996,JPO



**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☒ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.